

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-14862
(P2002-14862A)

(43) 公開日 平成14年1月18日 (2002.1.18)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 A 5 B 0 1 7
12/14	3 1 0	12/14	3 1 0 K 5 B 0 7 5
13/00	3 5 1	13/00	3 5 1 Z 5 B 0 8 2
15/00	3 3 0	15/00	3 3 0 D 5 B 0 8 5
17/30	1 2 0	17/30	1 2 0 B 5 B 0 8 9
審査請求 未請求 請求項の数5 OL (全 9 頁)			

(21) 出願番号 特願2000-193871 (P2000-193871)

(22) 出願日 平成12年6月28日 (2000.6.28)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 山崎 重一郎

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74) 代理人 100094145

弁理士 小野 由己男 (外2名)

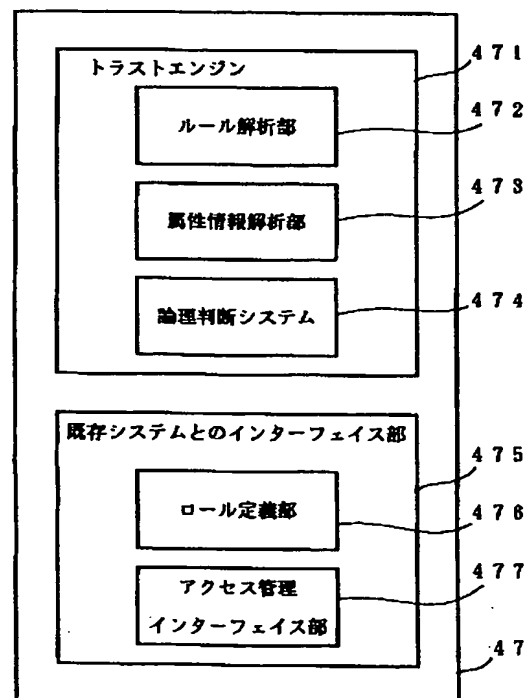
最終頁に続く

(54) 【発明の名称】 情報アクセス制御装置および情報アクセス制御方法

(57) 【要約】

【課題】 広域的に分散した個人情報に対するアクセス権限を、その個人情報の所有者本人の意志に基づいてコントロールすることを可能とし、情報プライバシー権を確保する。

【解決手段】 個人情報の所有者から受け付けたアクセスポリシーをルール解析部431によって解析し、外部アクセス者から送信されてくる属性証明書の内容を属性情報解析部432によって解析し、論理判断システム433によりこの外部アクセス者に対するアクセス権限をロール定義部451で定義されたロールとして割り当て、アクセス管理インターフェイス部452によりアクセス制御してデータを利用させる。



【特許請求の範囲】

【請求項1】 個人情報を含むデータベースを格納する記憶手段と、

前記データベース内の個人情報に対するアクセス権限を設定するためのアクセスポリシーを、前記個人情報の所有者から受け付けるアクセスポリシー受付手段と、前記アクセスポリシー受付手段で受け付けたアクセスポリシーを格納するアクセスポリシー記憶手段と、前記アクセスポリシー記憶手段に格納されているアクセスポリシーに基づいて、外部からのアクセス者に対して前記個人情報へのアクセスを制御するポリシーエンジンと、を備える情報アクセス制御装置。

【請求項2】 前記アクセスポリシー記憶手段およびポリシーエンジンは、前記記憶手段内に格納されているデータベースの情報を入出力制御するプロキシサーバ内に設定されている、請求項1に記載の情報アクセス制御装置。

【請求項3】 個人情報を含むデータベースを格納するデータサーバ上のデータを、インターネットを介してアクセスしてくる外部アクセス者にプロキシサーバを介して利用させる際の情報アクセス制御方法であって、前記データベース内の個人情報に対するアクセス権限を設定するためのアクセスポリシーを、前記個人情報の所有者から受け付けて、前記プロキシサーバ上に格納するアクセスポリシー受付段階と、

外部アクセス者からのアクセスがあった場合に、前記プロキシサーバ内のアクセスポリシーを解析して、前記外部アクセス者のアクセス権限を判別するアクセスポリシー解析段階と、

解析したアクセス権限に基づいて前記外部アクセス者に対して前記データベース内の個人情報を利用させるアクセス制御段階と、を備える情報アクセス制御方法。

【請求項4】 アクセスポリシー受付段階で受け付けるアクセスポリシーは、個人情報に対するアクセス権限をアクセスルールとして定義したポリシーデータに前記個人情報の所有者による電子署名を付加したポリシー証明書でなる、請求項3に記載の情報アクセス制御方法。

【請求項5】 前記ポリシーデータは、公開鍵証明書などで認証可能な属性情報に対応付けてアクセス権限を定義したものである、請求項4に記載の情報アクセス制御方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、データベース中の個人情報保護を目的とする情報アクセス制御装置および情報アクセス制御方法に関する。

【0002】

【従来の技術】 昨今のインターネットの普及に基づいて、インターネット上に個人情報が分散的に存在するようになってきている。たとえば、個人情報を含んだデー

タ群を擁するデータベースシステムがインターネットを介してアクセス可能な状態となっている。このような個人情報については、個人情報の所有者本人に情報プライバシー権が存在すると考えられ、この情報プライバシー権の保護を観点とした問題が深刻になってきている。

【0003】 個人情報に関する情報プライバシー権は、「自己情報管理権」と定義され、自己の情報を自分でコントロールできる権利とされている。したがって、前述したようにインターネット環境で分散的に存在する個人情報は、個人情報の所有者本人がそれぞれアクセス権についてコントロールすることができるように構成されていることが好ましい。

【0004】 しかしながら、通常のデータベースシステムでは、データベースへのアクセス権限の管理は、データベース管理者が行うように設計されており、データベース中に含まれている個人情報の所有者本人が、自己の情報に対するアクセス権限をコントロールするように構成されていない。このため、個人情報の所有者にとっては、データベース中に含まれる個人情報が意志に反して公開されることが不都合である場合が生じる。また、データベース管理者にとっては、データベース中に含まれる個人情報を保護するために、守秘責任と運用負荷が大きくなるという問題がある。

【0005】

【発明が解決しようとする課題】 本発明は、広域的に分散した個人情報に対するアクセス権限を、その個人情報の所有者本人の意志に基づいてコントロールすることを可能とし、情報プライバシー権を確保することを目的とする。

【0006】

【課題を解決するための手段】 本発明に係る情報アクセス装置は、個人情報を含むデータベースを格納する記憶手段と、データベース内の個人情報に対するアクセス権限を設定するためのアクセスポリシーを、個人情報の所有者から受け付けるアクセスポリシー受付手段と、アクセスポリシー受付手段で受け付けたアクセスポリシーを格納するアクセスポリシー記憶手段と、アクセスポリシー記憶手段に格納されているアクセスポリシーに基づいて、外部からのアクセス者に対して個人情報へのアクセスを制御するポリシーエンジンとを備える。

【0007】 ここで、アクセスポリシー記憶手段およびポリシーエンジンは、記憶手段内に格納されているデータベースの情報を入出力制御するプロキシサーバ内に設定することが可能である。また、本発明に係る情報アクセス制御方法は、個人情報を含むデータベースを格納するデータサーバ上のデータを、インターネットを介してアクセスしてくる外部アクセス者にプロキシサーバを介して利用させる際の情報アクセス制御方法であって、データベース内の個人情報に対するアクセス権限を設定するためのアクセスポリシーを、個人情報の所有者から受

け付けて、プロキシサーバ上に格納するアクセスポリシー受付段階と、外部アクセス者からのアクセスがあった場合に、プロキシサーバ内のアクセスポリシーを解析して、外部アクセス者のアクセス権限を判別するアクセスポリシー解析段階と、解析したアクセス権限に基づいて外部アクセス者に対してデータベース内の個人情報を利用させるアクセス制御段階とを備える。

【0008】ここで、アクセスポリシー受付段階で受け付けるアクセスポリシーは、個人情報に対するアクセス権限をアクセスルールとして定義したポリシーデータに個人情報の所有者による電子署名を付加したポリシー証明書で構成することができる。また、ポリシーデータは、公開鍵証明書などで認証可能な属性情報に対応付けてアクセス権限を定義したものとすることができる。

【0009】

【発明の実施の形態】〔概略構成〕本発明の1実施形態が採用されるシステムについて図1にその概略構成を示す。個人情報の所有者は、情報所有者端末1によってインターネットへの接続が可能である。この情報所有者端末1は、個人情報の所有者が利用可能なパーソナルコンピュータによって構成できる。

【0010】外部アクセス者は、クライアント端末2によってインターネットへの接続が可能となっている。このクライアント端末2も同様にして、外部アクセス者が利用可能なパーソナルコンピュータで構成できる。データベースを管理する情報システム4は、インターネット3を介して情報所有者端末1、クライアント端末2、その他の端末とデータのやり取りを行うことが可能となっている。

【0011】情報システム4は、少なくとも、個人情報を含むデータベース43、データベース43内のデータ検索システムを含むデータサーバ42、情報システム4とインターネット3間のデータの入出力を行うプロキシサーバ41を備えている。

〔情報所有者端末〕情報所有者端末1では、データベース43に含まれている個人情報に対するアクセス権限を設定するためのアクセスルール作成環境11、電子署名を行うための秘密鍵を管理する秘密鍵管理部12、アクセスルールとそのアクセスルールの対象となる個人情報識別と電子署名とを合成したポリシー証明書を作成するポリシー証明書作成部13、インターネットとの接続を行うための通信ソフトなどとなるインターネット接続部14などを備えている。

【0012】ポリシー証明書作成部13で作成されるポリシー証明書の一例を図3に示す。ポリシー証明書5は、アクセスルール作成環境11で作成されたアクセスルール51と、データベース43内の個人情報を特定する個人情報識別52と、秘密鍵管理部12で管理される秘密鍵で暗号化された電子署名53とから構成される。アクセスルール51、個人情報識別52、電子署名53

は、ITU-T X.509規格に基づいて、それぞれ識別子としてDNを備える一意名が付される。

【0013】アクセスルール51は、たとえば、外部アクセス者が提示する属性証明書に記載される属性と、データやサービスへのアクセス権限に関するロールとの対応であり、どのような属性に対してどのようなロールを与えるかを設定することで構成できる。アクセスルール51の一例を図4に示す。

【0014】図4では、ディレクトリ“https://www.a.b/usr/local/apache/htdocs/subarea/”に対するアクセス制御として、外部アクセス者が提示する属性があるパターンを持つ場合には、メンバーとしてのロールを与えるというアクセスルールを記述したものである。このディレクトリ“https://www.a.b/usr/local/apache/htdocs/subarea/”が、個人情報識別52となる。

【0015】この例では、〈if〉の〈cond〉節で、外部アクセス者の提示する属性証明書〈CLIENT#AC〉に対して、パターンマッチングを行い、条件を満たしたものである。〈then〉節で定義されたロールが与えられる。属性証明書の組織名“CLIENT#AC#DN#O”が“Fujitsu, Ltd.”にマッチングし、かつ部署名“CLIENT#AC#DN#OU”が“Staff”または“NML”にマッチングする場合に、member (can#read, can#modify, can#delete)というロールを与えることとする。このことにより、属性証明書の組織名および部署名がマッチングした場合に、この外部アクセス者に対して、読取・変更・削除を許可するアクセス権限が与えられる。

【0016】ポリシー証明書51に電子署名を付加する場合には、“POLICY CERTIFICATE”の欄の次に、“POLICY CERTIFICATE SIGNATURE”の欄を設け、秘密鍵によって暗号化された電子署名のデータを配置する。

〔プロキシサーバ〕プロキシサーバ41は、情報所有者端末1から送信されてくるポリシー証明書5を受け付けるポリシー受付部44、ポリシー証明書5の内容を記憶するポリシー記憶部45、ポリシー記憶部45の内容に基づいてアクセス制御を行うポリシーエンジン47とを備えている。

【0017】ポリシーエンジン47は、ポリシー受付部44で受け付けたポリシー証明書の内容を解析し、ポリシー証明書に含まれるアクセスルールに基づいて外部アクセス者2のアクセス権限を割り当てるためのトラストエンジン471と、データベース43内のデータに対するアクセス制御を行うための既存システムとのインターフェイス部475とを備えている。

【0018】トラストエンジン471は、ポリシー証明書5に含まれるアクセスルール51を解析するためのルール解析部472、外部アクセス者の属性を解析するための属性情報解析部473、属性情報解析部473で特定した外部アクセス者の属性とルール解析部472で解析したアクセスルールに基づいて外部アクセス者に対す

るルールを割り当てる論理判断システム474で構成される。

【0019】外部アクセス者は、データベース43内のデータへのアクセスを行うために、自己の属性を示した属性証明書と、本人であることを証明するための公開鍵証明書とをプロキシサーバ4に送信する。属性証明書は、一定の認証機関によって外部アクセス者がもっている属性を証明するものであって、ITU-T X.509属性証明書に準じたデータ形式で構成され、識別子としてDNを付した一意名のデータとすることができる。

【0020】公開鍵証明書は、ネットワーク上における本人認証を行うものであって、ITU-T X.509公開鍵証明書に準じたデータ形式で構成され、識別子としてDNを付した一意名のデータとすることができる。外部アクセス者から送信される属性証明書および公開鍵証明書のうち、公開鍵証明書は、SSL (Secure Sockets Layer) またはTSL (Transport Layer Security) などのユーザ認証のレイヤで評価される。ここで本人認証がなされた場合には、Secure API (Application Program Interface) を通じて外部アクセス者2から送信されてくるデータがプロキシサーバ47内のトラストエンジン471に入力される。このうち、属性証明書のデータは属性情報解析部473に送信され、そのデータ内容の解析が実行される。

【0021】属性証明書の構造の一例を図7に示す。ここでは、ITU-T X.509 Attribute Certificate として定義された属性証明書の例であって、ここでの属性とルールとの対応を定義することによって、ポリシー証明書内のアクセスルールを設定することができる。論理判断システム474では、属性情報解析部473で解析した外部アクセス者の属性と、ルール解析部472で解析したアクセスルールとから、外部アクセス者に対して割り当てるアクセス権限を判定し、対応するルールの割り当てを行う。

【0022】既存システムとのインターフェイス部475中のルール定義部476は、ポリシー証明書内で用いられるルールの定義を予め行うものである。ルールは、データやサービスへのアクセス権限の集まりに対する名前を定義するものであって、たとえば、個人の病歴に関する情報を管理しているシステムにおいて、「主治医」というルールに対して、個人の病歴の参照やカルテの作成や記述の追加など、主治医に関する個人情報への一定のアクセス権限の総体を割り当てるように設定できる。したがって、ルール定義部476において、アクセス権限とルールとを対応させたテーブルを作成し、このテーブルを管理する。

【0023】アクセス管理インターフェイス部477は、論理判断システム474の判定した外部アクセス者2のルールと、ルール定義部476で管理するテーブルに従ってアクセス権限を判定し、外部アクセス者による

データベース43へのアクセスを制御する。

〔基本動作〕プロキシサーバ47の基本動作を図8に示す。

【0024】ステップS1では、個人情報の所有者からポリシー登録の要求があったか否かを判別する。情報所有者端末1からポリシー登録の要求があったと判断した場合には、ステップS2に移行する。ステップ2では、情報所有者端末1からのポリシー登録の受付処理を実行する。ステップS3では、外部アクセス者2からのデータベース43へのアクセス要求があったか否かを判別する。クライアント端末2からのアクセス要求があった場合には、ステップS4に移行する。ステップS4では、アクセスルールに基づいてアクセス制御を行ってクライアント端末2に対してデータベース43を利用させる。

【0025】〔ポリシー登録〕個人情報の所有者によるポリシー登録要求があった場合のポリシー登録処理を図9に示す。ステップS11では、情報所有者端末1から送信されるポリシー証明書5を受け付ける。ポリシー証明書5は、前述したように、アクセスルール51、個人情報識別52、電子署名53から構成されたものとしてすることができる。

【0026】ステップS12では、電子署名53を解析する。たとえば、情報所有者の秘密鍵によって暗号化された電子署名を公開鍵によって復号化することによって、電子署名53を復元することができる。ステップS13では、電子署名53の内容により正常に個人認証がなされたか否かを判別する。個人認証が正常になされた場合にはステップS13に移行し、個人認証に失敗した場合にはステップS16に移行する。

【0027】ステップS14では、ポリシー証明書5内のアクセスルール51の解析を実行する。ここでは、前述したようなアクセスルール51を個人情報識別52とともにポリシー証明書5から抽出する。ステップS15では、ポリシー証明書5から抽出したアクセスルール51を個人情報識別52とともにポリシー記憶部45に格納する。

【0028】ステップS16では、個人認証に失敗した旨の表示を情報所有者端末1側に送信し処理を終了する。

〔アクセス制御〕図8ステップS4におけるアクセス制御の動作について図10に示す制御フローチャートと、図11に示すデータフローチャートに基づいて説明する。

【0029】ステップS21では、SSLプロトコルによるハンドシェイクを実行する。この場合、図11に示すように、クライアント端末2側からサーバに対してアクセス対象を指定したSSLハンドシェイク要求を行う。これに対応して、サーバ側からSSLハンドシェイク応答を行うことにより、クライアント端末2とサーバとのセッションを確立する。ここでは、SSLプロトコル中に、ク

クライアント端末2から送信されてくる公開鍵証明書の認証のネゴシエーションを行い、外部アクセス者の個人認証を行ってからセッションを確立する。外部アクセス者の個人認証に成功した場合には、Secure API を通じてプロキシサーバ47のトラストエンジン471内にその情報が送信される。個人認証に失敗した場合には、この旨の通知をクライアント端末2側に送信し、再度アクセスの実行を促す。

【0030】ステップS21では、SSLハンドシェイク処理の実行を行っているが、TLSプロトコルによるクライアントサーバのセッションを確立するように構成することもでき、クライアント端末2の環境に応じてSSL/TLSプロトコルのいずれにも対応可能とすることもできる。ステップS21においてクライアント端末2とサーバ側とのセッションが確立した場合にはステップS22に移行する。ステップS22では、クライアント端末2に対して属性証明書要求を送信する。

【0031】ステップS23では、クライアント端末2から属性証明書が送信されてきたか否かを判別する。クライアント端末2から属性証明書が送信されてきたと判断した場合には、ステップS24に移行する。ステップS24では、属性証明書の解析を行う。クライアント端末2から送信されてくる属性証明書は、前述したようにITU-T X.509標準に準拠したデータ形式とすることができ、また、IETF-PKIX 標準に準拠するデータ形式とすることも可能である。ここでは、それぞれの属性証明書のデータ形式に基づいて解析することにより、外部アクセス者の属性を判別することが可能となる。

【0032】ステップS25では、属性証明書を解析した結果と、アクセス要求のあった個人情報識別52に付随するアクセスルール51とを比較し、対応するロールの割り当てを行う。ここでは、前述したように、属性情報解析部473により解析した外部アクセス者の属性と、ルール解析部472により解析したアクセスルールの内容とを論理判断システム474によって判別して、外部アクセス者に対応するアクセス権限を与えるべくロールの割り当てを行う。ここで外部アクセス者に割り当てられるロールは、ロール定義部476で予め定義されたものである。割り当てられたロールは、ロール証明書としてクライアント端末2に送信される。同時に、このクライアント端末2からのアクセス要求に対して、割り当てられたロールに相当するアクセス権限が設定される。

【0033】ステップS26では、クライアント端末2

からの実際のデータアクセスがあったか否かを判別する。ここでは、アクセス要求のあった個人情報識別52に対するデータ表示要求やデータダウンロード要求などが、クライアント端末2から送信されてきた場合には、データアクセス要求があったと判断してステップS27に移行する。

【0034】ステップS27では、外部アクセス者に割り当てられたロールに基づいてアクセス制御を行い、データベース43内のデータを利用させる。ここでは、個人情報識別52によって特定される個人情報の一部または全部を読み取ることの可・不可、変更することの可・不可、削除することの可・不可などのアクセス制御をアクセス管理インターフェイス部477で行い、外部アクセス者に対するアクセス制限を行う。

【0035】ステップS28では、外部アクセス者からのアクセスが終了したか否かを判別する。クライアント端末2からのアクセス終了の旨の信号を受信した場合には、この処理を終了する。

【0036】

【発明の効果】本発明によれば、広域的に分散して存在する既存のデータベースに存在する個人情報へのアクセス制御を、個人情報の所有者本人がアクセスルールとして定義することができ、情報プライバシー権の保護を維持することが可能となる。外部アクセス者に対して、自動的にアクセス権限を判別させることにより、データベース管理者による運用負荷を低減できる。さらに、アクセス権限の判別は、個人情報の所有者本人が登録したアクセスルールに基づくものであり、その判断ロジックを確実にトレースすることが可能であるため、データベース管理者の守秘責任に基づく負荷も低減することができる。

【図面の簡単な説明】

【図1】本発明の概略構成図。

【図2】情報所有者端末の概略構成図。

【図3】ポリシー証明書の概略構成を示す説明図。

【図4】ポリシー証明書の一例を示す説明図。

【図5】プロキシサーバの概略構成図。

【図6】プロキシサーバの概略構成図。

【図7】属性証明書の一例を示す説明図。

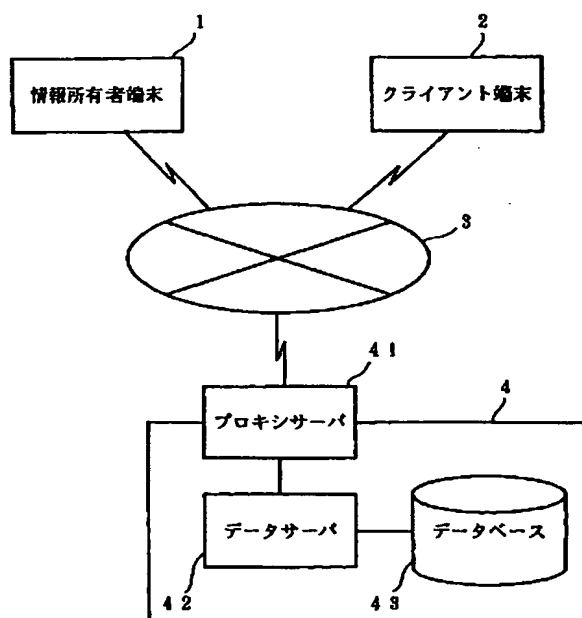
【図8】サーバ側の動作を示すフローチャート。

【図9】サーバ側の動作を示すフローチャート。

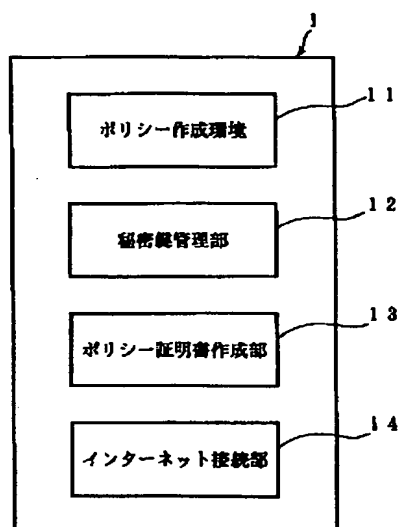
【図10】サーバ側の動作を示すフローチャート。

【図11】アクセス時におけるデータフローチャート。

【図1】

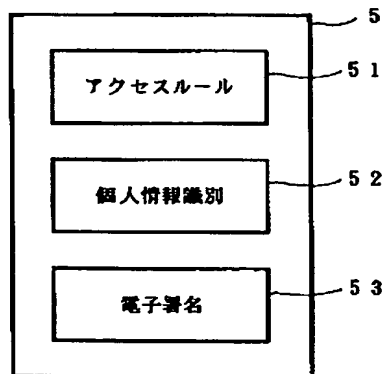


【図2】

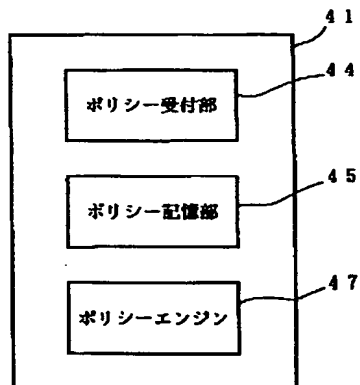


【図6】

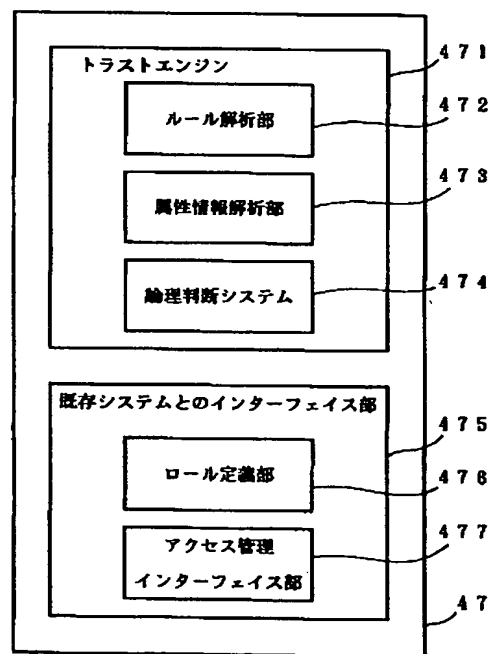
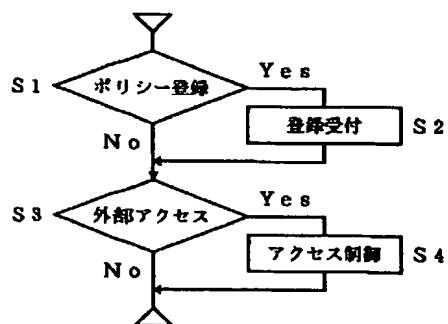
【図3】



【図5】



【図8】



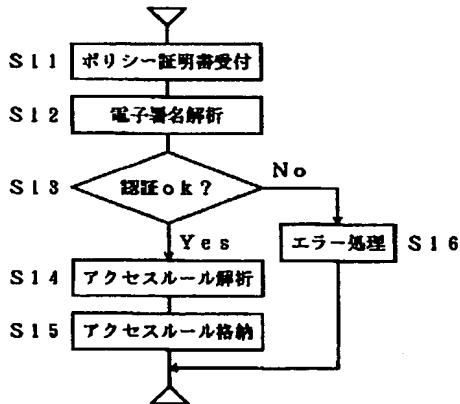
【図4】

```

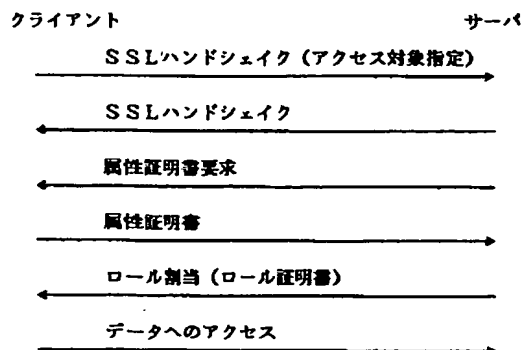
----- BEGIN POLICY CERTIFICATE -----
<directory https://www.a.b/usr/local/apache/htdocs/subarea/>
  <if>
    <cond>
      % {CLIENT AC DN O} eq " Fujitsu, Ltd" and
      % {CLIENT AC DN OU} in ( " Staff " : " NML " )
    </cond>
    <then>
      member(can read, can modify, can delete)
    </then>
  </if>
</directory>
----- END POLICY CERTIFICATE -----
----- BEGIN POLICY CERTIFICATE SIGNATURE -----
MIIDNjCCAp+gAwIBAgIBATANBgkqhkiG9w0BAQQFADCBqTELMAKGA1UEBhMCWFky
FTATBgNVBAGTDFNuYWt1IERlc2VydDETMDEGA1UEBxNKG93b2UgVG93bjEXMBUG
A1UEChMOU25ha2UgT2lsLCBMdGQxHjAcBgNVBAsTFUNlcnRqZmljYXR1IEF1dGhv
cm10eTEVMBMGA1UEAxMMU25ha2UgT2ls1ENBMR4wHAYJKoZIhvcNAQkBFg9 YUBz
----- END POLICY CERTIFICATE SIGNATURE -----

```

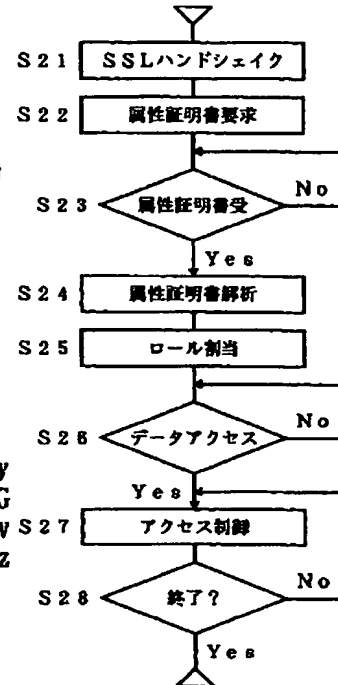
【図9】



【図11】



【図10】



【図7】

```

AttributeCertificate ::= SEQUENCE {
    acinfo      AttributeCertificateInfo.
    signatureAlgorithm AlgorithmIdentifier.
    signatureValue BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
    version      AttCertVersion DEFAULT v1.
    holder       Holder.
    issuer       AttCertIssuer.
    signature    AlgorithmIdentifier.
    serialNumber CertificateSerialNumber.
    attrCertValidityPeriod AttCertValidityPeriod.
    attributes   SEQUENCE OF attribute.
    issuerUniqueID UniqueIdentifier OPTIONAL.
    extensions   Extensions OPTIONAL
}

AttCertVersion ::= INTEGER {v1(0), v2(1)}

Holder ::= SEQUENCE {
    baseCertificateID [0] issuerSerial OPTIONAL.
    -- the issuer and serial number of
    -- the holder's Public Key Certificate
    entityName [1] GeneralName OPTIONAL.
    -- the name of the claimant or role
    objectDigestInfo [2] objectDigestInfo OPTIONAL
    -- if present, version must be v2
}

objectDigestInfo ::= SEQUENCE {
    digestedObjectType ENUMERATED {
        publickey (0),
        publickeyCert (1),
        otherObjectTypes (2) }
    -- otherObjectTypes MUST NOT
    -- MUST NOT be used in this profile
    otherObjectTypeId OBJECT IDENTIFIER OPTIONAL.
    digestAlgorithm AlgorithmIdentifier.
    ObjectDigest BIT STRING
}

AttCertIssuer ::= CHOICE {
    oldForm GeneralNames.
    newForm [0] SEQUENCE {
        issuerName GeneralNames. OPTIONAL.
        baseCertificateID [0] issuerSerial OPTIONAL.
        objectDigestInfo [1] objectDigestInfo OPTIONAL
        -- at least one of issuerName, baseCertificateID or --
        -- objectDigestInfo must be present --
        -- if newForm is used, version must be v2
    }
}

IssuerSerial ::= SEQUENCE {
    issuer GeneralNames.
    serial CertificateSerialNumber.
    issuerUID UniqueIdentifier OPTIONAL
}

AttCertValidityPeriod ::= SEQUENCE {
    notBeforeTime GeneralizedTime.
    notAfterTime GeneralizedTime
}

Although the Attribute syntax is defined in [PKIXPROF], we repeat
the definition here for convenience.

Attribute ::= SEQUENCE {
    type AttributeType.
    values SET OF AttributeValue
    -- at least one value is required --
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY

```


フロントページの続き

Fターム(参考) 5B017 AA03 BA07 CA16
5B075 KK43 KK54 KK63 UU08
5B082 EA11 HA08
5B085 AE13 AE23 AE29 BC01 BG07
5B089 GA19 GB02 JB22 KA17 KB13
KC58